# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/757,058 | 01/08/2001 | John E. Brezak | MS1-679US | 6566 |

22801 7590 06/13/2006

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

| EXAMINER | |
|---|---|
| TRAN, ELLEN C | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2134 | |

DATE MAILED: 06/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/757,058 | BREZAK ET AL. | |
| | Examiner | Art Unit | |
| | Ellen C. Tran | 2134 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *21 February 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-15,18-26 and 28-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15,18-26 and 28-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

***Detailed Action***

1. This action is responsive to communication: amendment filed on 21 February 2006 the original application was filed on 8 January 2001.

2. Due to amendment claims 1-15, 18-26, and 28-35 are currently pending in this application. Claims 1, 8, 13, 18, 23, 24, 29, 32, and 34 are independent claims. Claims 16, 17, and 27 have been canceled. Claims 1, 5, 8, 24, 29, 32, and 34 have been amended. The amendment to the claims is accepted.

***Response to Arguments***

3. Applicant's arguments listed and spoken during the telephone interviews of 31 January 2006 and 6 February 2006 as well as present in the remarks sections that:

- the amendment to the claims removes all 112 rejections made and ,

- the new claims are not taught by the cited references, have been considered but they are not persuasive where noted below or they are moot when an independent claim, as in the case of 1, 8, 24, 29, 32, and 34 was amended and a new rejection applied.

In response to applicant's arguments that claim 18 is allowable; the Office disagrees, as shown below claim 18 is taught by Stoltz et al. U.S. Patent No. 6,615,264.

In response to applicant's argument pertaining to removal of the 112 rejection from claims 1-7; the Office disagree because claim 1 is missing the following limitation which was added at some point to independent claims 8, 24, and 29: "retrieving the requested credential from a database of credentials; a marshaler configured to marshal the requested credential and return the marshaled credential to the low-level-credential-application, wherein marshaling performed by the marshaler is characterized by converting a description of the high-level

credential into a format recognizable as a low-level credential" to remove the 112 the step of retrieving the high-level credential from somewhere (a database) before it is marshaled needs to be added to claim 1.

In response to applicant's argument that all claims are allowable the Office disagrees, where, no modification was made to the independent claims the previously provided rejection is shown below.

In response to applicant's amendment to independent claims 1, 8, 24, 29, 32, and 34, the below rejection shows these claims are not allowable.

### *Claim Rejections - 35 USC § 112*

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-7 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. Claim 1 is indefinite because the text in the claims it is unclear where the process gets the high-level credential, i.e. an application another device, another processor, a database.

7. To expedite a complete examination of the instant application the claims rejected under 35 U.S.C. 112 above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the statutory categories of the invention.

*Claim Rejections - 35 USC § 102*

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

9. **Claims 13-15 and 32-35** are rejected under 35 U.S.C. 102(e) as being anticipated by Olden U.S. Patent No. 6,460,141 (hereinafter '141).

**As to independent claim 13, "A method for authenticating a user to a network, the method comprising: obtaining a request for a credential to authenticate the user to access a resource within the network, wherein the resource requires an appropriate credential before the user may access the resource; locating the appropriate credential; returning the appropriate credential to the resource within the network, so that the resource allows the user to access such resource; wherein the obtaining, locating, and returning are performed without user interaction so that the user need not be aware that such steps are being performed"** is taught in '141 col. 25, lines 29-39.

**As to dependent claim 14, "further comprising repeating the obtaining, locating, and returning for a different network that is authenticated using a different credential"** is taught in '141 col. 23, line 55-67 and col. 25 lines 5-20.

**As to dependent claim 15,** this claim is directed to a computer-readable medium of the method of claim 13 and is rejected along the same rationale.

**As to independent claim 32, "An application programming interface (API) method comprising"** is taught in '141 col. 3, lines 39-61;

**"receiving a CredUI-promptfor-credentials call having a set of parameters comprising a TargetName, Context, AuthFlags, and Flags; retrieving the parameters from the call to determine a specified resource; obtaining a credential; associating the credential with the specified resource; persisting the credential into a database while maintaining the credential's association with the specified resource"** is shown in '141 col. 9, line 27 through col. 10, line 36 (Note in '141 col. 9, lines 27-34 teach "During a request for the CustomerAccountApplication the enabled Web server 20 processes the ACCESS application function 84 to determine accessibility to the application 88. Once a user 68, that is a service contract customer, is granted access, the customer account application uses the API server 16 to determine the different application functions 84 (this is interpreted to have the same meaning as resources) to which the customer has access rights, and returns the correct interface which supports the function set").

**As to dependent claim 33, "wherein the set of parameters further comprises an indicator of a data structure containing customized information to display in conjunction with a user interface"** is disclosed in '141 col. 10, 32-39.

**As to independent claim 34, "An application programming interface (API) method comprising: receiving a CredUI-promptfor-credentials call having a set of parameters comprising a TargetName, UserName, Password, and Flags; retrieving the parameters from the call to determine a requesting application"** is taught in '141 col. 8, line 51 through col. 9, line 34 (Note in addition to what was explained above the API client can have additional

functions added by the administrator which also cause parameters to be retrieved from the call such as the user level) ;

**"obtaining a low-level credential from a user, wherein such credential includes a username and a password; returning the low-level credential to the requesting application"** is shown in '141 col. 7, lines 26-41.

**As to dependent claim 35, "wherein the set of parameters further comprises an indicator of a data structure containing customized information to display in conjunction with a user interface"** is disclosed in '141 col. 10, lines 17-39.

10. **Claims 18-19, 21, and 22** are rejected under 35 U.S.C. 102(e) as being anticipated by Stoltz et al. U.S. Patent No. 6,615,264, (hereinafter '264).

**As to independent claim 18, "A credential management architecture, comprising: a trusted computing base (TCB) that has 111 access to persisted credentials, the TCB being configured to interact with an entrusted computing layer (UTCL) that accesses the persisted credentials via the TCB"** is shown in '264 col. 5, lines 56-64 and col. 7, lines 19-23;

**"the TCB comprises: a credential management module configured to receive requests from the UTCL for a high level credential for a resource, the high level credential being associated with a user and not being username-and-password based authorization"** is disclosed in '264 col. 8, lines 57-65;

**"a credential database associated with the user, wherein credentials are persisted within the database; the credential management module being configured to retrieve credentials from the database"** is taught in '264 col. 9, lines 35-37.

**As to dependent claim 19, "architecture as recited claim wherein credential**

**management module is further configured to marshal a requested high-level credential and return the marshaled credential to the UTCL"** is disclosed in '848 col. 4, line 16-34.

**As to dependent claim 21, "A computer-readable medium having computer-executable instructions that, when executed by a computer, employ an architecture as recited in claim 18"** is shown in '264 col. 4, lines 16-22.

**As to dependent claim 22, "An operating system embodied on a computer-readable medium having computer-executable instructions that, when executed by a computer, employ an architecture as recited in claim 18"** is disclosed in '264 col. 5, lines 51-55.

*Claim Rejections - 35 USC § 103*

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. **Claims 1-12, 20-26, and 28-31** are rejected under 35 U.S.C. 103(a) as being unpatentable over Stoltz et al. U.S. Patent No. 6,615,264, (hereinafter '264) in further view of King et al. U.S. Patent No. 6,934,848, (hereinafter '848).

**As to independent claim 1, "A method for accommodating a legacy application, the legacy application having provisions for a low-level credential authorization model which employs username-and-password based authorization, the method comprising:"** is taught in '264 col. 7, line 41 through col. 8, line 6 "FIG. 2 illustrates authentication and session

management components and their interactions according to an embodiment of the invention. Network terminal 202 is a human interface device (HID) (e.g., HIDs 821, 822 and 823). An HID has, as examples of its functions, the task of displaying output of services to a user and obtaining input to services from the user. Network terminal 202 has the ability to respond to a command (e.g., display command) received from, for example, a software program (e.g., services 230-238, authentication manager 204 and session manager 206) executing on a computational service provider (e.g., computers 710, 711, 712, 713, and 714). The input received from a user is forwarded to, for example, a service that is fulfilling a user request. More than one server can execute the services that comprise a session. For example, in session 208, service 230 is executing on server 210, services 232 and 234 are executing on server 212 and services 236 and 238 are executing on server 214. A user may access a system (e.g., a server, a session, a service and a network terminal) by initiating a login or other authentication mechanism (e.g., smart card, biometric data, etc.). A separate authentication module 240 may be utilized for each authentication mechanism. During login, the user is validated by an authentication module 240. The authentication modules 240 communicate with authentication manager 240 where a user may be associated with a particular session";

**"obtaining a request from a high-level credential authorization model for a high-level credential to be provided by the legacy application, wherein the high-level credential authorization model does not employ username-and-password based authorization"** is shown in '264 col. 8, lines 57-65 "Authentication modules 240 each have the option of accepting or declining responsibility for a particular connection. Authentication modules 240 may base their decision on other available system resources or settings (e.g., from services 230-238,

external databases, etc.). In one or more embodiments, an authentication module 240 can be configured to accept all users all of the time, to only accept connections with smart cards, or to only accept users with pseudo tokens, for example";

the following is not taught in '264 "**marshalling the requested high-level credential, the marshalling is characterized by converting a description of the high-level credential into a format recognizable as a low-level credential by the legacy application employing a low – level credential authorization mode**" however '848 teaches "Processing the first sign-on further comprises: establishing the secure session from a client machine to a server machine using the digital certificate, wherein the digital certificate represents an identity of the client machine or a user thereof; storing the digital certificate or a reference thereto at the server machine; establishing a session from the server machine to a host system using a legacy host communication protocol; passing the stored digital certificate or the reference from the server machine to a host access security system; authenticating, by the host access security system, the identity using the passed digital certificate or a retrieved certificate which is retrieved using the reference; using the passed or retrieved digital certificate to locate access credentials for the user; accessing a stored password or generating a password substitute representing the located credentials; and using the stored password or the generated password substitute to transparently complete the first sign-on to a secure legacy host application executing at the host system" in col. 4, lines 16-34.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a security and access management method taught in '264 to include an authentication means that accommodates legacy applications. One of ordinary skill in the art would have been

motivated to perform such a modification because there are instances in a SSO application that different security credentials are required by a user see '848 (col. 3, lines 17 et seq.). "Furthermore, there may be cases where it would be desirable to provide different sign-on credentials during a secure host access session, following the initial sign-on. As an example, it may be necessary for the current legacy host application user's supervisor to sign on to the legacy application, such as when a special transaction requiring supervisory authority is to be performed. Or, it may happen that different security credentials are required for a user when he wishes to change from one legacy host application to another. As another example, there may be applications for which it is necessary or desirable to force the user to re-authenticate himself by providing his security credentials again (for example, by swiping his Smart Card through a Smart Card reader) at defined points, such as when a new application transaction begins. Because establishing a secure connection between the client and the TN3270 server or Web application server using a security protocol such as SSL is relatively expensive in terms of computation and networking resources, the performance overhead incurred in re-starting the session in order to supply a different certificate that signifies different user credentials makes this a less-than-optimal solution. Thus, a technique is needed which enables changing the user's credentials within the scope of an on-going secure session. Neither the prior art nor the related invention provide this capability".

**As to dependent claim 2, "further comprising, after the obtaining, seeking the requested credential in a database of credentials"** is taught in '264 col. 9, lines 35-37 "Authentication module 240 verifies the challenge response with user information retained in

authentication database 218, for example, information supplied by the user and information that is generated during authentication".

**As to dependent claim 3, "wherein a high-level credential is a credential selected from a group composed of X.509 Certificates and bio-metrics"** is shown in '264 col. 7, lines 61-65.

**As to dependent claim 4 "wherein the marshaled credentials appear to be a conventional username/password pair to the legacy application"** is disclosed in '848 col. 4, lines 16-34.

**As to dependent claim 5, "wherein marshaling comprises: obtaining the requested high-level credential; converting the requested high-level credential to generate a low-level credential that represents the requested high-level credential while appearing to be a conventional username/password pair to the legacy application"** is taught in '848 in col. 4, lines 16-34.

**As to dependent claim 6, "A method as recited in claim 1, wherein the legacy application never has access to the high-level credential"** is shown in '848 col. 18 line 60 through col. 19, line 8 "which then makes it more difficult for a security exposure to extend beyond the scope of a single host application. As will be obvious to one of skill in the art, the server determines whether the legitimate certificate holder sent the subsequent sign-on by using the public key 374 from the transmitted certificate to decrypt the AUTHINFO parameter value. Upon decrypting the value, the server compares the concatenated information to the server's copy of the random seed and sequence number, and to the application ID sent on the APPLID

parameter. In this manner, the server can authenticate the changed credentials during the on-going session in a manner that is transparent to the legacy host application".

**As to dependent claim 7, "A computer-readable medium having computer-executable instructions that, when executed by a computer, perform a method as recited in claim 1"** is taught in '264 col. 4, lines 16-23 "An embodiment of the invention can be implemented as computer software in the form of computer readable code executed on a general purpose computer such as computer 100 illustrated in FIG. 1".

**As to independent claim 8, "In a computing environment where certain processes have a provision for low-level credentials but have no provision for high-level credentials, wherein a provision for low-level credentials employs username-and-password based authorization while a provision for high-level credentials does not employ username-and-password based authorization, a method for accommodating such processes comprising:"** is taught in '264 col. 9, lines 18-26 "Authentication modules may be structured for any mechanism that verifies the identity of the user to the system. A key or password known only to the user, or biometrics information can be used to authenticate the user";

**"obtaining a request for a credential from a process, wherein the requested credential is a high-level credential, which is not username-and-password based;** is shown in '264 col. 8, lines 57-65;

**"retrieving the requested credential from a database"** is disclosed in '264 col. 9, lines 35-37;

**"converting the requested high-level credential into a format approximating a low-level credential and representative of the requested high-level credential; returning the converted credential to the process"** is taught in '848 col. 4, lines 16-34.

**As to dependent claim 9, "wherein a high-level credential is a credential selected from a group composed of X.509 Certificates and bio-metrics"** is taught in '264 col. 7, lines 61-65.

**As to dependent claim 10, "wherein the converted credentials appear to be a conventional username/password pair to the process"** is shown '264 col. 7, lines 61-65.

**As to dependent claim 11, "wherein the process never has access to the high-level credential"** is disclosed in 848 col. 18, line 60 through col. 19, line 8

**As to dependent claim 12, "A computer-readable medium having computer-executable instructions that, when executed by a computer, perform a method as recited in claim 8"** is taught in '264 col. 4, lines 16-23.

**As to dependent claim 20. An architecture as recited in claim 18, wherein the marshaled credentials appear to be a conventional username/password pair to the UTCL"** is taught in '848 col. 4, lines 16-34.

**As to independent claim 23, "An apparatus comprising: a processor; a marshaler executable on the processor to: obtain a high-level credential wherein a high-level credential is employed in an authorization model which is not username-and-password based authorization"** is shown in '264 col. 8, lines 57-65;

**"convert the high-level credential to generate a representation of the high-level credential that is formatted as a low-level credential so that it appears to be a conventional username/password pair"** is disclosed in '848 col. 4, lines 16-34.

**As to independent claim 24, "An accommodation system comprising:"** is taught in '264 col. 7, line 41 through col. 8, line 6;

**"a request obtainer configured to obtain a request for a high-level credential from a low-level-credential-application, wherein low-level credentials utilizes username-and-password based authorization while high-credentials utilizes username-and-password based authorization while high-level credentials do not employ username-and-password based authorization"** is shown in '264 col. 8, lines 57-65;

**"a credential retriever configured to retrieve the requested credential from a database of credentials"** is disclosed in '264 col. 9, lines 35-37;

**"a marshaler configured to marshal the requested credential and return the marshaled credential to the low-level-credential-application, wherein marshaling performed by the marshaler is characterized by converting a description of the high-level credential-application employing a low-level credential authorization model"** is taught in '848 col. 4, lines 16-34.

**As to dependent claim 25, "wherein a high-level credential is a credential selected from a group composed of X.509 Certificates and bio-metrics"** is shown in '264 col. 7, lines 61-65.

**As to dependent claim** 26, **"wherein the marshaled credentials appear to be a conventional username/password pair to the legacy application"** is disclosed in '848 col. 4, lines 16-34.

**As to dependent claim** 28, **"wherein the low-level-credential-application never has access to the high-level credential"** is taught in '848 col. 18 line 60 through col. 19, line 8

**As to independent claim 29, "A system for authenticating a user to a network, the system comprising:"** is shown in '264 col. 7, lines 6-25 "The computer systems described above are for purposes of example only";

**"a request obtainer configured to obtain a request for a high level credential to authenticate the user to access a resource within the network wherein the resource requires an appropriate credential before the user may access the resource, wherein ahigh-level credential do not utilize username-and-password based for high-level credential authorization"** is disclosed in '264 col. 8, lines 57-65;

**"a credential retriever configured to retrieve the appropriate high-level credential from a database of credentials"** is taught in '264 col. 9, lines 35-37;

**"a credential marshaler configured to generate a representation of the high-level credential formatted as a low-level credential so that it appears to be a conventional username/password pair to a low-level-credential-application wherein a low-level credential utilizes username-and-password based authorization; a credential returner configured to return the marshaled credential to the resource within the network, so that the resource allows the user to access such resource"** is shown in '848 col. 4, lines 16-34;

**"wherein the obtainer, retriever, marshaller and returner are further configured to operate without user interaction"** is disclosed in '848 col. 3, lines 51-53 "Another object of the present invention is to provide this technique in a manner that does not require the user to re-identify himself".

**As to dependent claim 30, "An operating system comprising a system as recited in claim 29"** is taught in '264 col. 5, lines 51-55.

**As to dependent claim** 31, **"A network environment comprising a system as recited in claim 29"** is shown in '264 col. 5, lines 56-64.

**Conclusion**

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 8:00 am to 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques H. Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ECT

Ellen Tran
Patent Examiner
Technology Center 2134
6 June 2006

JACQUES H. LOUIS-JACQUES
PRIMARY EXAMINER